UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/551,674	10/03/2006	Richard Kabzinski	60136-0011	5546

29989 7590 10/04/2010

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/04/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/551,674	KABZINSKI ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to amendment and remarks filed on May 6, 2010. The remarks filed have been entered and made of record. Claims 29-54 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 6, 2010 has been entered

Response to Arguments

Applicant's arguments filed on May 6, 2010 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 29-54 applicants argued, that cited prior art (CPA) [Thibadeau U. S. Patent 7,036,020] does not *teach or suggest "blocking means" for blocking access to a security partition that stores an operating system, at least the reason that because Thibadeau does not describe a security partition that stores an operating system. Moreover, because Thibadeau does*

not describe such blocking means, Thibadeau also does not teach or suggest that such blocking means are "deployed along the chain of components that connect the CPU to the storage device" comprising the security partition, as now recited in Claims".

This is not found persuasive. The system of cited prior art teaches a system and method for promoting security method in computer system that involves partitioning portion of storage device to form security partition and limiting access to portion of storage device by operating system of computer. In that system a portion of storage device is partitioned to form a security partition, which has an authority record and data set associated with the authority record. An access to security partition of storage device is limited by the installed operating system of computer. The methods and systems include a storage device having security partition data 32 and at least one authority record, such as authority record 34, associated with the security partition data 32. These security partition data 34 and authority records 34, 36, 38 are contained in a security partition of the storage device 30. In practice a distinction can be made between an external authority source and an internal authority source. This means that while certain data, such as a private key, can be written, the data are not read by any external process, because they are defined as hidden.

(Fig.1-4, col.4 line 37 to col.6 line 16).

As a result, cited prior art does implement and teach a system that relates to securing access in a computer system. Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 29-54 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 29-52 are rejected under 35 U.S.C. 102(e) as being anticipated by Thibadeau U. S. Patent 7,036,020.

2. Regarding Claim 29, Thibadeau teaches and describes a security system for securing access to an operating system of a computer having at least a host central processing unit (CPU), computer memory means used by the host CPU to load programs from the operating system in order to operate the computer, a storage device for storing data to be used by the computer, and a chain of components connecting the CPU to the storage device, the security system comprising: a security partition formed in the storage device, the operating system being stored in the security

partition; and blocking means for interpreting communication and selectively blocking data access between the host CPU and the security partition, wherein the blocking means are deployed along the chain of components that connect the CPU to the storage device (Fig.1-4, col.4 line 37 to col.6 line 16).

3. Regarding Claim 42, Thibadeau teaches and describes a method for securing access to an operating system of a computer, the computer having at lest a host central processing unit (CPU), a storage device for storing data to be used by the computer, a chain of components connecting the host CPU to the storage device, and memory used by the host CPU to load programs from the operating system in order to operate the computer and storage device, the method comprising: forming a security partition in the storage device; storing the operating system in the security partition; and at a first component deployed along the chain of components connecting the host CPU to the storage device, intercepting communications and selectively blocking data access between the host CPU and the security partition (Fig.1-4, col.4 line 37 to col.6 line 16).

4. Claims 30-41 and 43-54 are rejected applied as above rejecting Claims 29, and 42. Furthermore, system of Thibadeau teaches and describes a system and method for securing access to an operating system of a computer, wherein:

As per Claim 30, each user of the computer has an associated access profile, each access profile comprising information indicative of the level of access to portions of the storage device permitted by a user, and the blocking means controlling access to the storage device by a user in accordance with the access profile associated with the user (col. 6 line 55 to col.8 line 35).

As per Claim 31, the security system is arranged such that at least two different data access profiles are defined; one access profile ascribing read and write access to said security partition, and the other access profile not ascribing write access to said security partition (col.6 line 55 to col.8 line 35).

As per Claim 32, said blocking means is independent and separately configurable of said host CPU (col.4 line 37 to col.6 line 16).

As per Claim 33, during operation of the operating system the security system is arranged to divert and write operating system files to a location different to the security partition so that normal operation of the operating system continues even though operating system files in the secure partition have not been updated (col.5 line 25 to col.6 line 16).

As per Claim 34, the security system is arranged to divert and write operating system files to a flash ROM (Fig.1-4, col.4 line 37 to col.5 line 50).

As per Claim 35, the security system is arranged to divert and write operating system files to an invisible partition formed in the storage device (col.5 line 15 to col.6 line 16).

As per Claim 36, further comprising authentication means for authenticating a user of the computer and associating the user with a prescribed access profile, said blocking means controlling subsequent access to the security partition in accordance with the access profile associated with the user(col. 6 line 55 to col.8 line 35).

As per Claim 37, said blocking means includes processing means for controlling operation of said blocking means (col.5 line 25 to col.6 line 16).

As per Claim 38, said blocking means is configured to block all access by the host CPU to the storage device before initialisation of the security system, and to selectively permit access

immediately after said initialisation in accordance with a respective access profile (col. 6 line 55 to col.8 line 35).

As per Claim 39, said authentication means enables a software boot of the computer to be effected only after correct authentication of a user, and said security system permits normal loading of the operating system during the start up sequence of the computer following said software boot (col.6 line 55 to col.8 line 35).

As per Claim 40, said blocking means is a security device physically deployed between an interface adapter and the storage device within a data access channel of the chain of components connecting the host CPU and the storage device (col.4 line 37 to col.6 line 16).

As per Claim 41, said blocking means is disposed as part of a bridging circuit (Fig.1-4, and col.4 line 37 to col.6 line 16).

As per Claim 43, further comprising associating each user with an access profile comprising information indicative of the level of access to portions of the storage device permitted by a user; and for each user, selectively blocking access between the host CPU and the security partition in accordance with the access profile defined for the user (col.5 line 25 to col.6 line 16).

As per Claim 44, further comprising defining at least two different access profiles, one access profile ascribing read and write access to data stored on said security partition, and the other access profile not ascribing write access to said security partition (col. 6 line 55 to col.8 line 35).

As per Claim 45, further comprising authenticating a user of the computer, and associating the user with an access profile after successful user authentication (col.5 line 15 to col.6 line 16).

As per Claim 46, said selective blocking comprises controlling access between the host CPU and the security partition independently of the host CPU (col.4 line 37 to col.6 line 16).

As per Claim 47, said selective blocking comprises totally blocking access to the storage device by the host CPU during initialisation of the computer, and intercepting all said access immediately after said initialisation and before loading of the operating system of the computer (col.6 line 55 to col.8 line 35).

As per Claim 48, including performing a software boot of the computer only after correct authentication of the user, and allowing normal loading of the operating system during the start up sequence of the computer after said software boot (col. 6 line 55 to col.8 line 35).

As per Claim 49, further comprising diverting and writing operating system files to a location different to the security partition during operation of the operating system so that normal operation of the operating system continues even though operating system files in the secure partition have not been updated (col.5 line 25 to col.6 line 16).

As per Claim 50, the operating system files are diverted and written to a flash ROM (Fig.1-4, col.4 line 37 to col.5 line 50).

As per Claim 51, the operating system files are diverted and written to an invisible partition formed in the storage device (Fig.1-4, col.4 line 37 to col.6 line 16).

As per Claim 52.including unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU (Fig.1-4, and col.4 line 37 to col.6 line 16).

As per Claim 53, the first component is a dedicated hardware device comprising a dedicated CPU for processing the intercepted communication and, based on the intercepted communications, determining whether to block data access between the host CPU and the security partition (col.4 line 45 to line 65, and col.9 line 13 to line 22).

As per Claim 54, the first component is a bridging circuit comprising logic for processing the intercepted communications and, based on the intercepted communications, determining whether to block data access between the host CPU and the security partition (col.4 line 45 to line 65, and col.9 line 13 to line 22)..

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
September 25, 2010
/Syed Zia/
Primary Examiner, Art Unit 2431